Workplace Alaska

Class Specification
Network Engineer

Created:	**AKPAY Code:**	**Class Code:**	RR3112N
05/18/2005 by Cheryl Evans	**Class Outline Cat:** A	**Class Range:**	NR 15
Finalized on:	**Approved by:**	**Class Status:**	Active

Category: Professional
Original Date: 05/18/2005

Class Title: Network Engineer
Use MJR Form: Alaska Railroad

Original Comments:

Subsequent Revision Dates/Comments:

Last Update: 11/19/2008 **EEO4:** 2 **SOC:** 15-1071 **Census:**

Last Update Comments:
Updated position description to include supervising employees and new reporting relationship.

Definition:
The Network Engineer's role is to ensure the stability and integrity of in-house voice, data, video and wireless network services. This is achieved by planning, designing, and developing local area networks (LANs) and wide area networks (WANs) across the organization, and supervising subordinate staff members. In addition, the Network Engineer will participate with the installation, monitoring, maintenance, support, and optimization of all network hardware, software, and communication links. This individual will also analyze and resolve network hardware and software problems in a timely and accurate fashion, and provide end user training where required.

Distinguishing Characteristics:

Examples of Duties:
Coordinates, installs, and tests operating systems, local area network, wide area network, IP-Telephony, video and wireless equipment. Ensures the stable operation of the in-house computer network. This includes planning, developing, installing, configuring, maintaining, supporting, and optimizing all network hardware, software, and communication links. Installs and configures software applications, messaging and printer systems. Manages servers related to network monitoring and reporting, security, and system usage and trending and archival requirements. Manages security solutions, including firewall, anti-virus, and intrusion detection systems and their distribution to the end-user desktop. Manages all network hardware and equipment, including routers, switches, hubs, and UPS's, and their configurations. Provides on-call technical support. Ensure network connectivity of all servers, workstations, telephony equipment, fax machines, and other network appliances.

Advises management and users on software and hardware solutions, or upgrades that improve systems and operations effectiveness for all network systems. May serve as the project manager while providing technical analysis of systems alternatives to users. May negotiate with vendors on pricing and other terms and conditions. Reviews ARRC network initiatives and ensures that solutions follow ARRC standards and align with Corporate technology strategies. Conducts research on emerging products, services, protocols, and standards in support of systems software procurement and development efforts.

Troubleshoots and resolves network problems. Initiates corrective action with vendor representatives as appropriate, opening trouble-tickets, if required, to bring in vendor support for resolution. This includes installing upgrades or patches and configuring and optimizing all network hardware, software, and communication links as part of resolution. The incumbent will also analyze and resolve end user hardware and software computer problems that have been escalated from the helpdesk, in a timely and accurate fashion, and provide end user training where required. Develops, implements and maintains policies, procedures, and associated training plans for network administration, usage, and disaster recovery.

Supervises and directs the activities and resources of Network Analysts. Coaches, mentors, and motivates subordinate staff and influences them to take positive action and accountability for their assigned work. Identifies and resolves issues and conflicts within and between various project assignments.

Manages configuration and connection security for all networks (LAN, MAN, WAN, VLAN, WLAN), the company Web site, the company intranet, and e-mail and digital-fax communications. Manages access policies and maintenance of systems that monitor and provide or restrict access to external systems and sites in accordance with ARRC policies and guidelines. Manages and ensures the access security of databases and data transferred both internally and externally. Coordinates with end user community for system outages related to upgrades, planned maintenance, or unscheduled problem resolution.

Deploys, manages and maintains all security systems for end user and system security, and their corresponding or associated software. This includes firewalls, intrusion detection systems, cryptography systems, and anti-virus software. Assists in design and implementation of disaster recovery plan, routines and schedules for networks, servers, and software applications. Designs, performs, and/or oversees penetration testing of all systems in order to identify system vulnerabilities. Assists in the development and execution of security plans for protection of corporate data from unauthorized internal or external access. Monitors server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interprets activity and makes recommendations for resolution This includes scrutinizing network traffic, establishing and updating virus scans, and troubleshooting. The incumbent will also analyze and resolve security breaches and vulnerability issues in a timely and accurate fashion, and conduct user activity audits where required.

Collaborates with executive management and department leaders to assess near- and long-term network capacity needs. Creates and maintains documentation as it relates to network configuration, network mapping, processes, and service records. Conducts research on

network products, services, protocols, and standards to remain abreast of developments in the networking industry. Practices network asset management, including maintenance of network component inventory and related documentation and technical specifications information.
Provides schematics, documentation, procedures, and guidance on network issues to users and internal staff.
Develops information to support Authorization for Expenditures (AFEs) for acquisition of computer equipment and software.
Performs other duties as assigned.
May be required to drive an ARRC vehicle.

Knowledge, Skills and Abilities:

FACTOR 1: Technical and Operational Knowledge

Thorough knowledge of methods, practices and techniques that enable the incumbent to function as the ARRC's technical authority on programs, systems, local area network, and wide area network is required.

Bachelor's degree in math or computer science is required. Five (5) years of equivalent work experience in an increasingly responsible network or systems administration position with a working technical knowledge of hardware, network, PC and Server operating systems, including Cisco routers, switches, and firewalls, HP Servers, Active Directory, Exchange Servers, Windows 9x- NT/2000–XP servers and workstations may substitute for the degree requirement. Two years of recent experience as a Network Engineer or a Network Analyst with Cisco hardware and software experience is required. Two years of recent experience as a system administrator on IBM OS400, UNIX and/or Microsoft systems that entailed significant emphasis on systems security is required. One year of supervisory experience is preferred. Certified Microsoft and/or Cisco Network Engineer is preferred.

Working technical knowledge of current network hardware, protocols, and standards, including Ethernet, IP Addressing, and Wireless 802.11x communications protocols is required. Must have extensive, recent hands-on hardware troubleshooting experience. Certifications in Cisco Networking (CCNA, CCNE), Microsoft Exchange Administrator, Microsoft (MCSA, MCSE) or equivalent experience is preferred. Voice and IP Telephony experience is a plus.

Must have a good understanding of the organization's goals and objectives. Must also have a thorough understanding of the functions of the Information Technology Department and a general knowledge of the functions of other ARRC departments for the purpose of responding to systems/network problems and providing guidance in the acquisition of hardware and software.

Must have knowledge of applicable data privacy laws and practices. Must have strong written and oral communication skills and the ability to present ideas in user-friendly language.

FACTOR 2: Analytical Skills & Impact

Uses judgment in resolving specific issues or problems and in the development and execution of security plans for corporate data. Must possess the ability to conduct research into security issues and products as required. Relies on extensive experience and judgment to plan and accomplish goals.

Must be able to analyze the software/hardware needs of all ARRC employees and determine the most effective approaches to improve systems and optimize hardware and software utilization. Must have the skills and ability to develop schematics, documentation, procedures, and provide guidance to ARRC users and internal staff. Must have the skills and ability to provide assistance in the development and execution of security plans for protection of corporate data from unauthorized internal or external access. Knowledge and skill required to review, evaluate, and recommend selection and acquisition of hardware and software for LAN, WAN, and personal computers.

The work affects daily computer operations throughout the ARRC.

Ability to conduct research into networking issues and products is required. Performs a variety of tasks, often simultaneously. A wide degree of creativity and autonomy is expected. Must have the ability to effectively prioritize and execute tasks in a high-pressure environment. Must have strong interpersonal skills and a strong customer service orientation. The incumbent must be highly self-motivated and directed with a keen attention to detail.

FACTOR 3: Supervision and Control

Incumbent is responsible for the supervision of two Network Analysts. The position works under the supervision of the VP Information, Technology and Telecommunications.

FACTOR 4: Communication

Communicates with ARRC employees for the purpose of coordinating and managing programs, systems and network operating software, resolution of system problems, providing documentation, schematics, flow charts, and training to staff and users on software solutions, system improvements, and operations effectiveness. Contacts are made with vendor representatives in the research and acquisition of solutions, software, hardware and the resolution of problems. Interacts and negotiates with vendors, outsourcers, and contractors to secure network products and services.
FACTOR 5: Working Conditions

Work is performed in a corporate office environment however; some travel may be required to locations throughout the rail belt. Work entails sitting for extended periods of time. Dexterity of hands and fingers is required to operate a computer keyboard, mouse, power tools, and to handle other computer components. Work requires on-call availability for 7 days on a rotating basis with other Information

Technology staff.
Lifting and transporting of moderately heavy objects (up to 50 lbs), such as computers and peripherals, is required occasionally.

Minimum Qualifications:

Bachelor's degree in math or computer science is required. Five (5) years of equivalent work experience in an increasingly responsible network or systems administration position with a working technical knowledge of hardware, network, PC and Server operating systems, including Cisco routers, switches, and firewalls, HP Servers, Active Directory, Exchange Servers, Windows 9x- NT/2000–XP servers and workstations may substitute for the degree requirement. Two years of recent experience as a Network Engineer or a Network Analyst with Cisco hardware and software experience is required. Two years of recent experience as a system administrator on IBM OS400, UNIX and/or Microsoft systems that entailed significant emphasis on systems security is required. One year of supervisory experience is preferred. Certified Microsoft and/or Cisco Network Engineer is preferred.

Extensive application support experience with HP OpenView, Microsoft Office Suite 2000, PIX firewall, Cisco Works, Norton Anti-Virus, and various filter and scanning utilities is required. Similar software experience may be substituted for firewall, anti-virus/security, and patching and sniffer software.

Working technical knowledge of current network hardware, protocols, and standards, including Ethernet, IP Addressing, and Wireless 802.11x communications protocols is required. Must have extensive recent hands-on hardware troubleshooting experience. Certifications in Cisco Networking (CCNA, CCNE), Microsoft Exchange Administrator, Microsoft (MCSA, MCSE) or equivalent experience is preferred. Voice and IP Telephony experience is a plus.

Required Job Qualifications:

(The special note is to be used to explain any additional information an applicant might need in order to understand or answer questions about the minimum qualifications.)

Special Note:

Minimum Qualification Questions:

Did you answer the above listed questions?